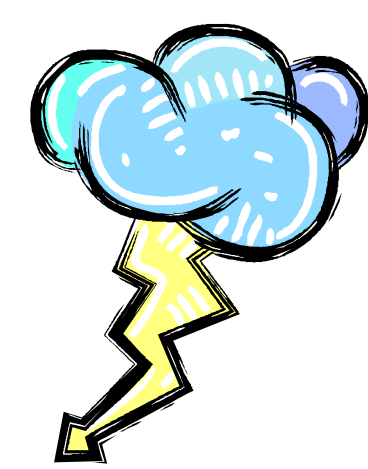


# CERIAS

the center for education and research in information assurance and security

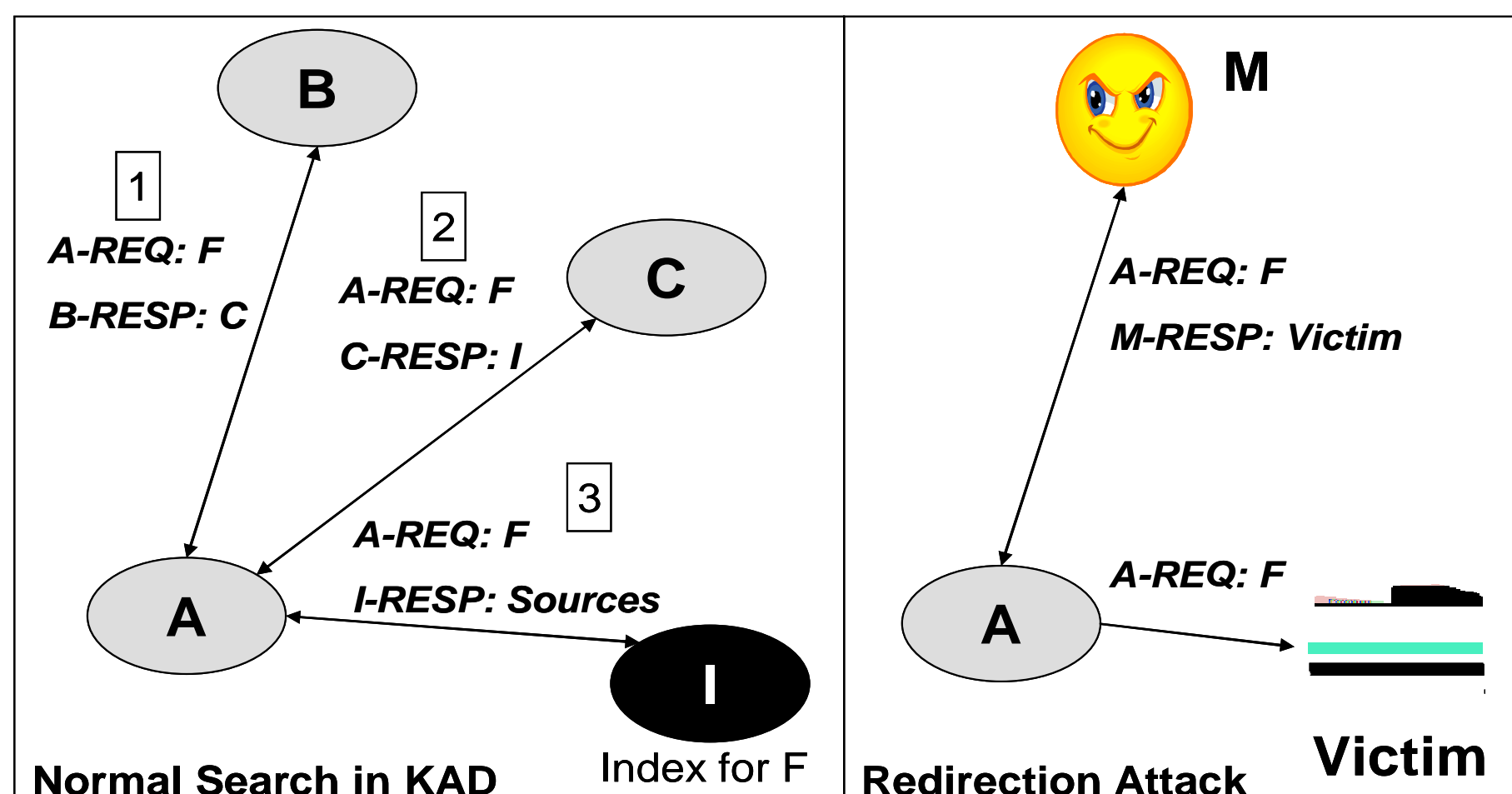
## Preventing DDoS Attacks with P2P Systems

Xin Sun, Ruben Torres, Sanjay Rao



### DDoS attacks are *feasible* with P2P Systems

- Ø Vulnerabilities commonly exist in the membership protocols of many P2P systems;
  - KAD, BitTorrent-DHT, Overnet, Gnutella, ESM...
- Ø DDoS attacks are feasible by exploiting those vulnerabilities;
- Ø Such attacks can be launched towards **any** hosts, even those do not participate in any P2P systems!



Exploiting KAD search mechanism to generate a *redirection* DDoS attack towards a host that's **not** part of KAD.

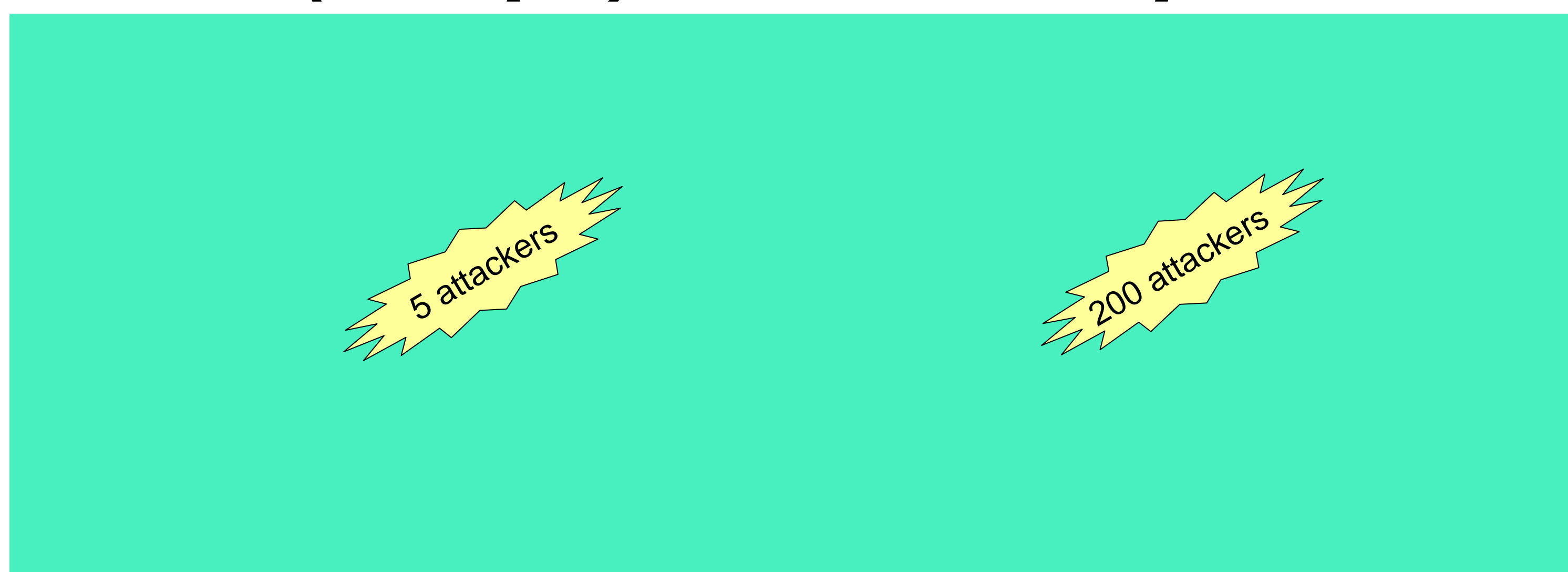


The large scale of P2P systems (>1M concurrent users) makes such DDoS attacks **huge magnitude (~Gbps)**, **hard to stop** and **hard to trace back**.

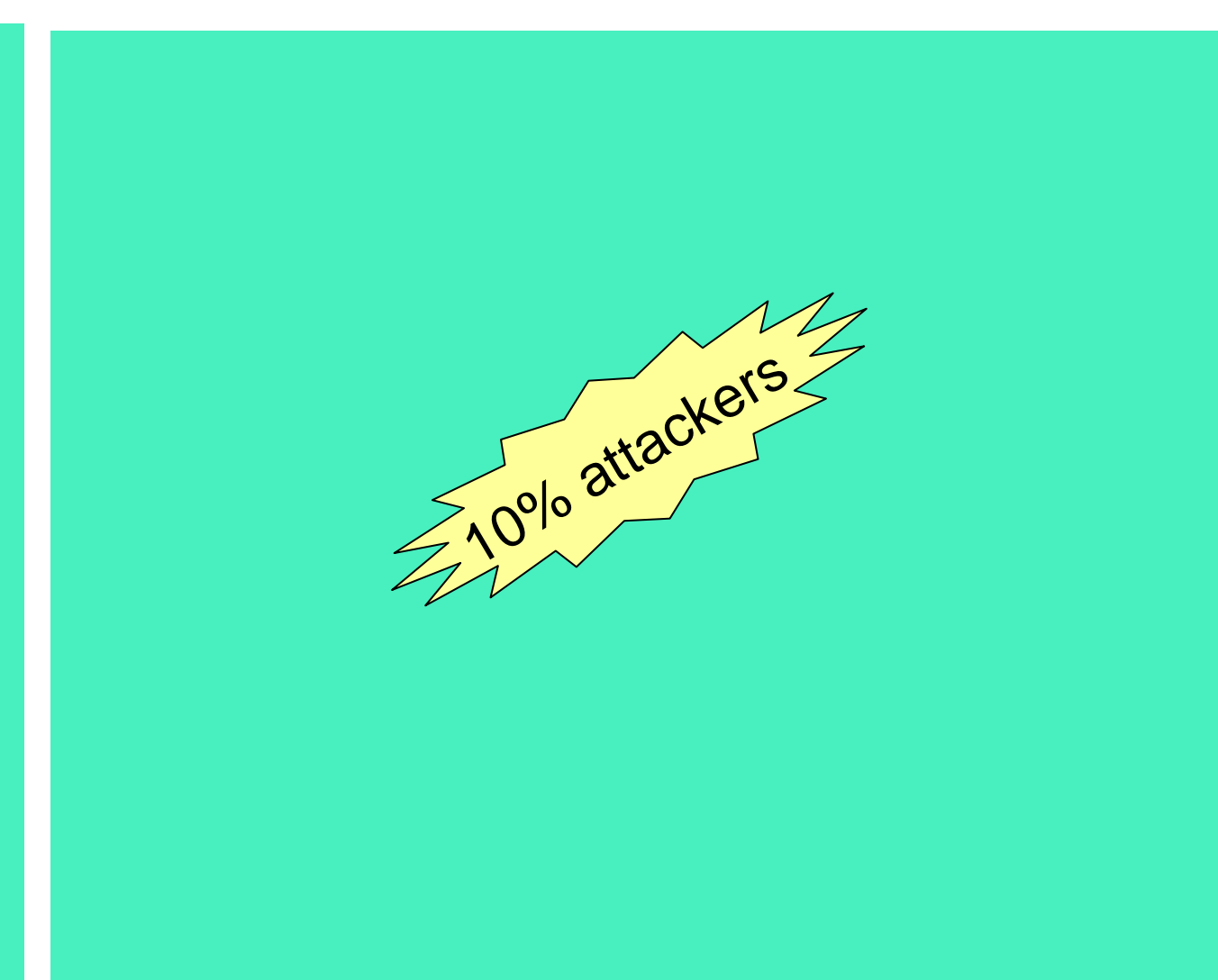
Ø Two different P2P systems are exploited:

- DHT-based **KAD**
- Gossip-based **ESM**

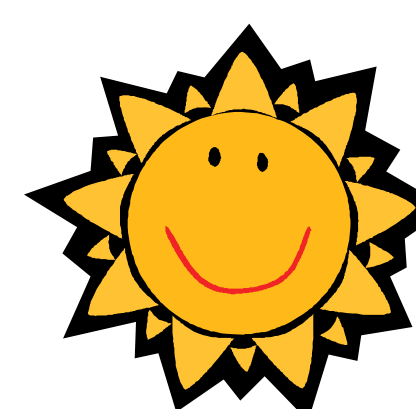
Ø Traffic seen by the victim is shown in the graphs.



KAD (File Distribution, *DHT*)



ESM (Broadcasting, *Gossip*)



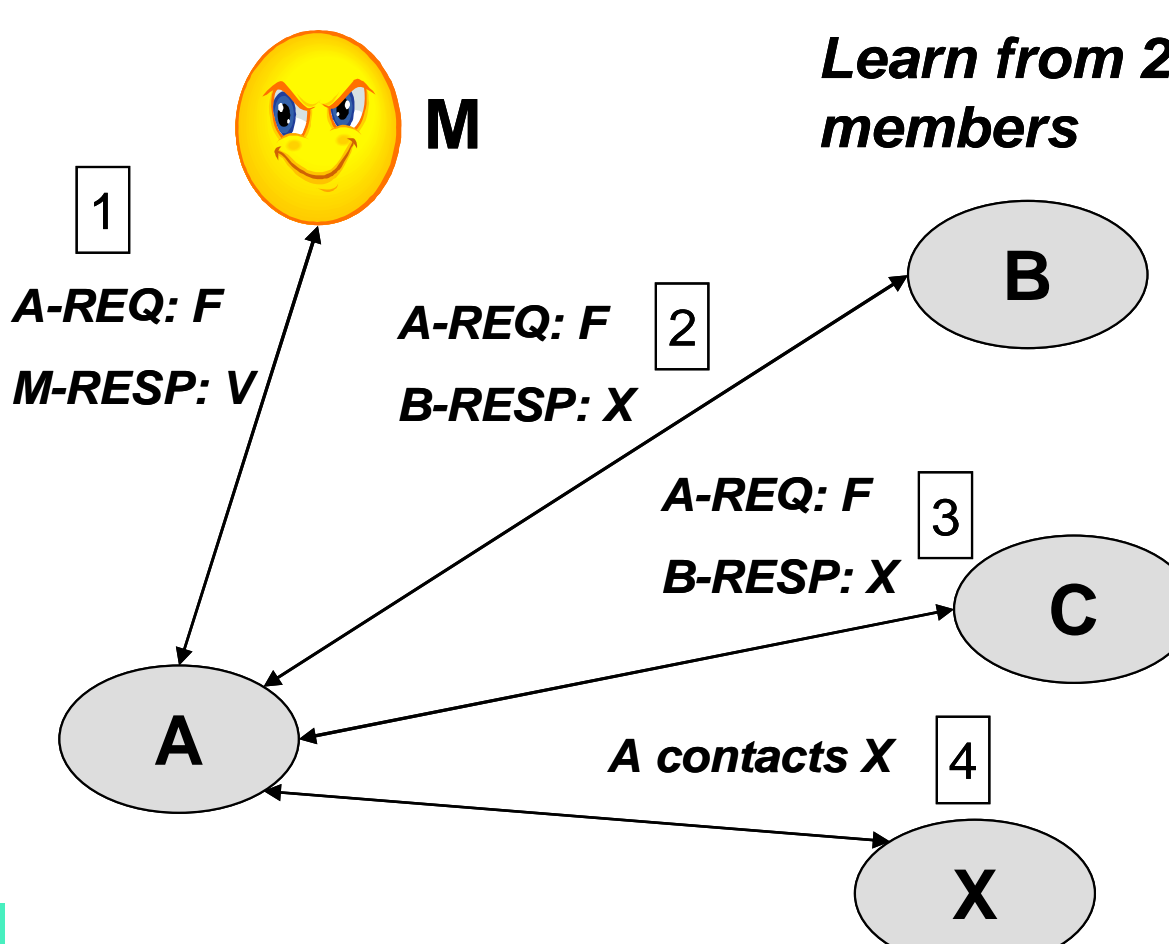
### Preventing such DDoS attacks through **Robust Membership Management**

#### Pull + Direct Validation

- Ø **Pull:** Any information conveyed by a member is always in response to a prior solicitation
- Ø **Direct Validation:** Immediately probe any new node learned through a third party before considering it as a neighbor.
- Ø **Pull + Direct Validation:** Neither of the two is enough by itself. Combine them for improved system robustness.

#### Validation through Multiple Sources

- Ø Nodes will not accept any information until learn from at least *K* members.



#### Bounding Logical IDs for a Physical ID

- Ø An attacker could repeatedly redirect an innocent node to a victim, using different logical IDs for the same physical ID, to amplify the attack.
- Ø Solution: bind the number of logical IDs for a physical ID a node can talk to.

